Release Notes

Version 6.5

N-able
MONITOR • MANAGE • OPTIMIZE®

August 17, 2007

Overview

N-central is a Web-based monitoring and management platform for Internet Protocol (IP) based networks providing notification and configuration options. Designed for the managed service provider servicing the small- to medium-sized business market, it allows for monitoring, management, and remote control of any Windows device.

You can access the N-central user interface from any supported Internet browser. The N-central server makes its user interface and status pages available by HyperText Transfer Protocol, Secure (HTTPS) over a Secure Socket Layer (SSL).

This document describes the new features, enhancements, upgrade requirements, and the known problems and solutions for this release.

Supported Hardware Platforms

N-central is designed and optimized to run on the following platforms:

- Supermicro SuperServer 6014P-8R 1U Dual
- HP ProLiant DL-360 G3, G4, and G5
- HP ProLiant DL-380 G3, G4, and G5
- HP ProLiant DL-140 G2
- IBM xSeries 335
- IBM xSeries 336
- Dell PowerEdge 2950

Before upgrading to N-central 6.5, ensure that your server meets the specifications published in the N-able Partner Resource Center's Certified Hardware lists.

New Hardware Minimum Requirements

Following are the hardware requirements:

- RAM: 3 GB
- Disk space: 72 GB

Advisory Notice

Warning! After the installation of N-central 6.5, ensure that you upgrade all Windows agents and probes in order to prevent the possibility of services transitioning to Stale or Misconfigured states.

Port Access Requirements

Central Server

You must have a firewall that is configured to allow access from the Internet to the following ports on the N-central server:

- TCP Port 22 - Secure Shell, which allows N-able to sign in and provide you with technical support and is also necessary for remote control (VNC Terminal Services of Remote Support Manager) functionality.
- TCP Port 80 (HTTP)
- TCP Port 443 (HTTPS)
- TCP Port 10000 (HTTPS)

Supported Browsers

N-central is supported on the following browsers:

- Internet Explorer, versions 6.0 and 7.0
- Mozilla Firefox, versions 1.5 and 2.0

Document Viewer Requirements

We recommend using the following version of Adobe Acrobat (as a minimum) to view N-central reports and documentation:

- Adobe Acrobat 7.0 (version 7.0.7)

Technical Documentation

All N-central technical documentation is available online either through the application's Help menu or through the Partner Center web sites.

New Features

The following provides a summary of the new features in N-central 6.5 and the changes to the existing features from the previous release.

Smart Folders

Smart Folders automate the process of setting up and managing devices.

Devices are associated automatically to Smart Folders when they are imported, manually added, or if the device class of the Smart Folder is changed. If you add a device class to a Smart Folder, devices of that class are immediately visible through that folder.

After Smart Folders are set up, you can start receiving notifications within minutes of the addition of a device to the system. In the same way as regular folders, Smart Folders can be associated to dashboards, notification profiles and service templates. As soon as Smart Folders are set up, the following happens without further user input:

- device status is displayed on dashboards,
- Service Organization level notifications are configured, and
- associated service templates are applied.

Folder Templates

Folder templates automate the process of setting up customers.

After folder templates are added to the system, N-central sets up new customers with a standardized set of dashboards, notification profiles, and folders automatically. When customers are added to the system, folder templates create folders and associate them with dashboards and notification profiles configured at the Service Organization level.

Because folder templates are set up at the Service Organization level, they make it very easy to set up and manage the association between specific folders, dashboards, and notification profiles.

You can use folder templates to create Smart Folders.

Service Templates

Service templates provide you with the ability to group and pre-configure services.

After setting up a service template, you can use it across all of your customers—this allows you to standardize how you monitor a specific application or network device. Service templates can be created at all levels of N-central 6.5 and applied to devices at any level. (Service templates created by SO Techs are the exception—these apply only to the SO Tech’s customers.)

Service templates also allow you to quickly make changes to monitoring across multiple customers. By changing the template at the SO level, all occurrences of that template across all of your customers will be changed.

You can use service templates to add services to devices or modify thresholds and properties of existing services.

With service templates, you can efficiently remove services from devices. If the monitoring done by a specific N-central service (or services) is no longer required, you can create a service template to remove those services from all devices for a specific customer, or for all of your customers.

You can clone a service template to copy a template and distribute copies of it to customers.

Service templates can be exported or imported.

Note: The service templates created in older versions of N-central can be converted into the new service template format. You must use the Devices menu to create a service from a device.

Asset Discovery and Management

N-central now provides improved asset discovery, importation, and management of discovered devices. Adding devices to the system is faster and easier with the following new features:

Agent-based Asset Management

Devices with Windows agents will automatically carry out asset discovery during the installation or upgrade of N-central without adding or initiating any discovery jobs.

Discovery Jobs

Both asset discovery and auto-discovery jobs have been redesigned to gather more comprehensive information about discovered devices. This information can include such things as discovery dates and times (for example, first discovery and most recent discovery) which are recorded for imported assets as well as the last logged-in user for Windows devices.

Discovered Device Mapping

Duplicating devices in the system as a result of asset discovery can now be avoided by mapping imported devices to devices that have already been entered manually.

Discovered Device Management

In addition to device mapping, discovered devices that are redundant or unnecessary can now be defined as “ignored” or deleted from the system. This improves organization and tracking of devices.

SNMP Community Strings

SNMP discovery is enhanced by default SNMP community strings that can be defined for an entire service organization and propagated to all customers. At the customer level, SNMP community strings can also be defined in the N-central UI and propagated to all of the customer's devices.

Auto Import

A new Auto Import feature incorporated into discovery jobs allows you to automatically import into the system any devices that are discovered by the job.

Automatic Assignment of Services

As part of the importation of devices during a discovery job, N-central automatically assigns services to devices based on the discovered assets found on the device. For example, the Disk (WMI) and Disk (SNMP) services will be automatically assigned to a discovered device that has local disk drives.

Probe IP Address

Probes now report their network address to the N-central server. You do not have to manually enter an address for probes.

Job Status Dashboard

The Job Status dashboard appears in the navigation pane under the NOC view. It displays the status of all jobs appropriate to the permission level of the user. Similar to the NOC view, there is an advanced filtering option which allows you to filter what you see based on selected customers or job types, as well as job status.

The Job Status dashboard is enabled by default for all administrator level accounts. It can be disabled in the account's profile.

Downtime Enhancements

N-central now provides the ability to schedule downtime periods on devices that extend overnight. You can also now place a device into downtime (change it to a Disconnected state) immediately. Downtime settings can also now be applied to all of a customer's devices in one procedure (useful for scheduled network maintenance). Downtime settings for all of a customer's devices are set in the same fashion as for a single device.

Activation Key Enhancement

Activation of N-central agents and probes has been enhanced by improvements to the activation keys including:

- Activation keys can now contain either an IP address or an FQDN.

- Using agent activation keys has been made easier by the addition of a key icon on the Device screen. To access the key, move your mouse over the icon and a window will be displayed showing the key. This can then be used to copy-and-paste the key.

Agent Installation and Uninstallation Enhancements

Installing and uninstalling agents on devices has been improved by the addition of a Local Agent check box. Select the check box to choose the probe to install the agent. Clear the check box to remove the agent.

New Default Elements

If you are new to N-central with version 6.5, you have been provided with default dashboards, service templates, and folder templates. These allow you to set up your system quickly and establish standardized monitoring for your customers.

For more information about default dashboards, service templates and folder templates, please refer to the online help.

Note: If you have upgraded to N-central 6.5, services, dashboards, and folders will remain configured exactly as they are. The new defaults will not be imported to your system.

Wizard Access Panel

N-central now provides quick access to performing common tasks. Through the new panel located in the bottom left corner of the UI, you can (depending on your permission level) Add Dashboard, Add Notification, and Add Service Template at the Product Administrator level, or access the Customer Wizard or Add Folder Template at the Service Organization level, or Add Probe, Add Discovery Job, Add Scripting Task, and Add Scheduled Report at the customer level. All this functionality is still available through the menu system but is supplemented by the panel.

Customizing State Priorities

The priority of state indicators on the dashboard can now be customized so that you can define the order in which states are displayed. You can do this through the new State Priority Management feature in the NAC.

Services

The following services have been added or revised in N-central 6.5:

Windows Event Log

The Windows Event Log service replaces the Event Log service. It allows you to monitor logs that are managed by the Windows Event Viewer. While the original

Event Log service was limited to only one instance of the service on a device at a time, the Windows Event Log can be used in multiple instances. When upgrading, previously defined Event Log tasks will be renamed as Windows Event Log tasks. The parameters of the new task will be modified to reflect all monitoring options of the original task.

Note: The default parameters for Windows Event Log cannot be modified through the NAC. You can use a service template in the UI to modify the parameters for this service and apply the service template (with the modified service) to devices as required.

WMI and SNMP Updates

When a service provider is not available, the services based on these technologies will report a Failed, not Misconfigured state.

WTS Removed – Merged into HTTP

The WTS service has been removed and its functionality merged into the HTTP service.

WTSS Removed – Merged into HTTPS

The WTSS service has been removed and its functionality merged into the HTTPS service.

Backup Exec – Updates

The Backup Exec service has been enhanced to include the Job History ID scan detail. In addition, it will not report on any discovered job that is still in progress or report on any discovered job more then once.

Windows Service

The new Windows Service service monitors the state and start up time of a specified Windows service including both manually configured and discovered service names.

Reports

The following reports have been added or revised in N-central 6.5:

Windows Event Log Reports

The new Windows Event Log report allows you to view a tabular log of monitored events. You can customize the log to report on selected devices as well as filtering the results based on different criteria.

Miscellaneous UI Improvements

View All

When a list of items continues on several pages (for example, Service Control), you can now click View All to allow all items in a list to be viewed on one screen.

NOC View

The navigation pane will now display a single NOC view. There is an advanced filtering option which allows you to filter what you see based on selected customers or notification types as well as status.

Miscellaneous NAC Improvements

Default Settings

The Default Settings screen in the NAC has been updated and simplified to provide a single set of endpoints. This feature verifies the settings before they can be changed.

Module Management

This has been moved to the Accounts>SO Customer screen in the NAC.

6.5 Enhancements

- Some tasks formerly identified as Misconfigured now display a Failed State. Tasks that cannot be completed due to WMI, SNMP or other services not being available (for example, in the case of a switch or router being turned off) now report a Failed state. This differs from the behavior in previous releases but more accurately reflects the true state of the service. You may wish to review your notification profiles to ensure that they are correctly configured to accomodate this change.
- The priority of state indicators on the dashboard can now be customized so that you can define the order in which states are displayed. The default setting is Default, Failed, Warning, Normal, Misconfigured, Stale, No Data, and Disconnected. In the NAC, you now have the ability to modify this order.
- The System Change service can be added to any device regardless of whether the device was manually entered into the system, discovered by network discovery, or discovered by asset discovery.
- The improved asset discovery feature now discovers only real network interfaces and ignores Packet Scheduler Miniport network interfaces.
- In the UI navigation pane, selecting a customer will now result in the dashboards associated with that customer being displayed.
- The Network Routable Address and IP Address/FQDN fields have been renamed Network Address in the following UI screens: Add/Edit Device, Add/Edit Probe, Configuration Summary Report, and Devices Report.
- Every instance of the Windows Event Log service will have a unique service identifier that will be used as a reference in notification e-mails.
- Windows probes now have the capability to monitor event logs on a device.
- When importing discovered assets, the Update Local Address option is now available.
- Notification repair scripts are now executed automatically following a database restore.
- Requesting an attended remote control session has been made easier and more efficient by improvements to the Remote Desktop Support - Contact Details screen.
- Documentation of the System Change service has been improved by the provision of configuration requirements notes.
- The capability to transfer tasks from Workgroup Windows probes to Network Windows probes has been enhanced by providing the ability to transfer multiple tasks in one operation.

Upgrading to N-central 6.5

Advisory Notices

Warning! Before upgrading to N-central 6.5, ensure you meet the system requirements or the upgrade will fail and there may be unrecoverable data loss or prolonged downtime.

Warning! After the installation of N-central 6.5, ensure that you upgrade all Windows agents and probes in order to prevent the possibility of services transitioning to Stale or Misconfigured states.

To upgrade, your central server must be running N-central 6.0 with Hotfix 3 (b6_0_0_431).

The N-central server must comply with the minimum hardware specifications. For more information, refer to Supported Hardware Platforms on page 2.

If you are upgrading using the CD method, you need a copy of the N-central 6.5 Upgrade CD. The CD is distributed as an .iso CD image and can be downloaded from the N-able Technologies Partner Resource Center Web page under Technical>Technical Support>Software Downloads.

Note: Instructions on how to burn the image to a CD are located in the Self Service Portal, Solution #277, *Burning an ISO image to a CD*.

If you are upgrading using the remote network install method, you can download a copy of the .nsp file from the Partner Resource Center Web page under Technical>Technical Support>Software Downloads.

If upgrading Hardware Probes manually, you need a copy of the N-central 6.5 installation CD for Network - Hardware Probes.

You must have a valid offline backup of an N-central server running the supported upgrade path version.

N-central 6.5 supports agents and probes from N-central 5.0 SP2 and greater. This can be checked through the System Health report in the NAC under the Services section.

Immediately following an upgrade to 6.5.0.x, the Windows Event Log Report will have no data (or incorrect data) in the Date-Time column for the duration of the initial data retention period. Once this period has completed, valid date/time data will be available.

Due to the merging of services, any existing WTS services will be renamed to HTTP services and any WTSS services will be renamed to HTTPS services.

You must perform the following three steps to upgrade to N-central 6.5:

1. Backing Up the Central Server — Important
2. Installing the N-central 6.5 Upgrade
3. Performing the Post-installation Steps

1. Backing Up the Central Server – Important

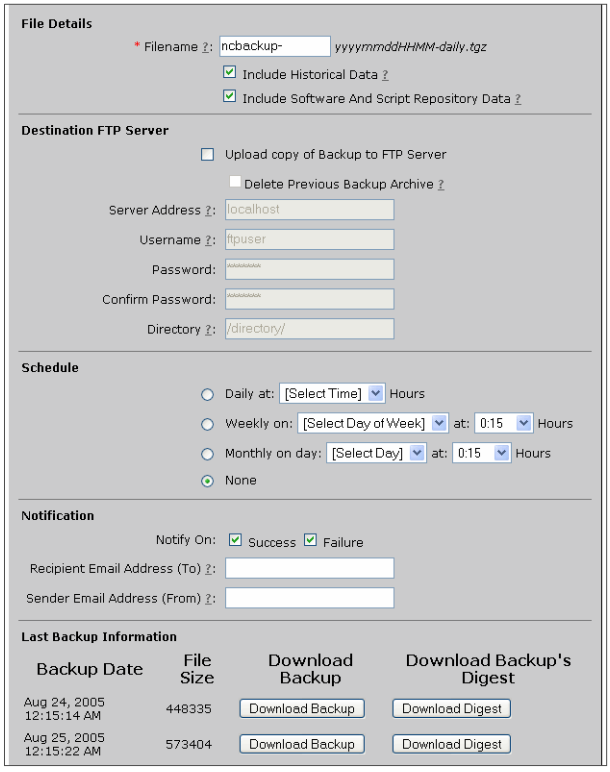
Warning! Before you perform the upgrade, you **must** back up the central server to a remote location. The backup will ensure that your data is protected in case of an error during the upgrade process.

The backup must be copied to a separate location. If the backup of your central server is stored on the central server, you may not be able to restore the backup in the event of a failure resulting in an unrecoverable data loss.

To back up the central server

1. In the NAC, select Setup>Database>System Backup.

   ↳ The System Backup screen appears.



2. In the Filename field, specify the name of the backup file.

   Note: N-central automatically appends the “yyyymmdd-HHMMSS.tgz” suffix to the specified name.

3. If required, select Include Historical Data.

   This option allows you to include the historical data in the backup, which is the bulk of the data used for reports.

   Note: It is recommended that you include the historical data; otherwise, all of the data that is used for reports will be lost.

4. If required, select Include Software And Script Repository Data.

   Note: You must select this if you intend to restore the software and script repositories.

   Warning! This step may considerably affect the size of the backup, depending on the combined size of the stored scripts and software packages in the repositories.

5. If you would like to upload a copy of the backup file to an FTP server:

   i. Select Upload copy of Backup to FTP Server.

   ii. If you would like to overwrite any existing backup files stored on the FTP server, select Delete previous backup archive.

   iii. In the Server Address field, specify the FQDN or IP address of the FTP server.

   iv. Specify the Username of the FTP server account.

   v. Specify the Password of the FTP server account.

   vi. In the Confirm Password field, specify the password again.

   vii. In the Directory field, specify the location on the FTP server in which you would like to save the backup file.

   For example: /home/test/backup/ (UNIX format)

6. In the Schedule section, select the time at which to regularly perform the backup or select None for no schedule.

7. If you would like to send a notification of the backup results:

   i. Select Success to send a notification upon the success of the backup.

   ii. Select Failure to send a notification upon the failure of the backup.

   iii. In the Recipient Email Address (To) field, specify the e-mail address of the notification recipient.

   iv. In the Sender Email Address (From) field, specify the e-mail address from which to send the notification.

8. Click Save Settings **or** Save Settings and Backup.

   ↳ If you clicked Save Settings, the specified settings are saved and the Setup screen appears. You can backup the database at a later date with the specified settings or the backup will be performed as scheduled in step 6.

   If you clicked Save Settings and Backup, your specified settings are saved, the database is backed up, and the Setup screen appears.

   During the backup, N-central creates a backup file and a backup digest file. The backup file contains all of the information needed to restore the system. The SHA1 file contains a SHA1 checksum of the backup file and verifies that the backup file is not corrupted. For example, it considers the backup file corrupt if any changes have been made to the backup file.

   Note: If you need to restore the database, you must ensure that the SHA1 checksum file is in the same location as the backup file.

   When the backup is complete, N-central lists the date and file size of the backup in the Last Backup Information section.

9. Wait for the system to send you a notification informing you of the backup success or failure.

   ↳ N-central sends the notification to the e-mail address that was specified in step 7.

   If the backup failed and the error cannot be corrected, contact N-able Technologies Technical Support.

   If the backup succeeded and you configured the backup to be uploaded to an FTP server, you can download it to a safe location. For example, you should download the backup to another safe location if you use the FTP server to maintain incremental backups and you would like to keep the current backup for a longer period. Perform steps in section: 2. Installing the N-central 6.5 Upgrade on page 15.

   If the backup succeeded and you did not configure it to be uploaded to an FTP server, manually download the backup image from the N-central server to a safe location and perform step 10 and step 11.

10. Under the Database heading, click System Backup.

    ↳ The System Backup screen appears and lists up to four of the most recent backups in the Last Backup Information section.

11. In the Last Backup Information section:

    i. Click Download Backup for the backup file that you would like to download.

    ii. If required, click the corresponding Download Digest button to download the backup digest file.

        ↳ The backup file is downloaded to your desktop.

2. Installing the N-central 6.5 Upgrade

You can upgrade to N-central 6.5 using any of the following methods:

- Install the upgrade from the CD. See To install the upgrade from the CD on page 15.
- Perform a remote network install of the upgrade. See To perform a remote network install of the upgrade on page 15.

Once you have upgraded to N-central 6.5, hotfix and service pack files will automatically be downloaded to a local repository for installation through the Version Management feature. See To upgrade N-central from the local repository on page 16

Warning! During the upgrade process, you must not reboot the central server even if it may appear unresponsive. If you are unsure of the status of the upgrade, please call N-able Technologies Technical Support, and they will be able to advise you of the current upgrade status.

To install the upgrade from the CD

1. In the NAC, select Central Server>Version Management.
   ↳ The View system information and install an upgrade screen appears.
2. Select Install upgrade from CD.
3. Insert the N-central 6.5 upgrade CD into the CD-ROM drive.
4. In the Notify this email address when complete field, specify the e-mail address of the recipient who is to receive the notification of the upgrade results.
5. Click Install.
   ↳ A confirmation screen appears.
6. Click Yes.
   ↳ You are signed out of the Administrator Console.

   You will receive an e-mail when the upgrade process has completed. If five hours have passed after the upgrade and you have not yet received a notification, contact N-able Technologies for assistance.

To perform a remote network install of the upgrade

1. In the NAC, select Central Server>Installation Settings.
   ↳ The Modify the installation settings screen appears.
2. In the Value column, increase the minutes to 30 for the UI Session Timeout.
3. Click OK.
   ↳ The Setup screen appears.

4. Under the Central Server heading, click Version Management.

   ↳ The View system information and install an upgrade screen appears.

5. Select Install upgrade remotely.
6. Do one of the following:
   - Insert the N-central 6.5 upgrade CD into your workstation and specify the Location of the upgrade file or click Browse to navigate to the file, which is located on the N-central 6.5 upgrade CD.

     The format of the upgrade file will be similar to: upgrade-cd-b<version>.nsp
   - Download a copy of the .nsp file from the Partner Resource Center Web page under Technical>Technical Support>Software Downloads and browse to navigate to the file.
7. In the Notify this email address when complete field, specify the e-mail address of the recipient who is to receive the notification of the upgrade results.
8. Click Install.

   ↳ A confirmation screen appears.

9. Click Yes.

   ↳ You are signed out of the Administrator Console.

   You will receive an e-mail when the upgrade process has completed. If five hours have passed after the upgrade and you have not yet received a notification, contact N-able Technologies for assistance.

To upgrade N-central from the local repository

Note: This feature is only available after N-central 6.5 has been installed and subsequent upgrade files are available.

1. In the NAC, select Central Server>Version Management.

   ↳ The Version Management screen appears.

2. Under the Install Upgrade heading, select the N-central upgrade (that has been downloaded to the local repository) you would like to install.

   Note: Upgrade files that have been downloaded but that you are not eligible to use will be displayed in the Install upgrade from local repository list but will not be accessible.

3. Click Install.

   ↳ The Upgrade Confirmation screen appears.

4. Click Confirm.

3. Performing the Post-installation Steps

After you have installed N-central 6.5, you must perform some post-installation steps. Table 1-1 Post-installation Checklist provides a checklist of these steps.

Advisory Notice

Warning! After the installation of N-central 6.5, ensure that you upgrade all Windows agents and probes in order to prevent the possibility of services transitioning to Stale or Misconfigured states.

Table 1-1: Post-installation Checklist

✓	**Installation CD (if applicable)**
	If you installed the upgrade from CD, ensure that the N-central 6.5 upgrade CD has been removed from the CD-ROM drive.
✓	**Verification**
	Verify the version of N-central by signing into the Administrator Console and selecting Version Management under the Central Server heading. The Associated Upgrades displayed must read Applied-update-6.5.0.xxx-b6_5_0_xxx, where xxx is a number.
	Verify that the Administrator Console configuration is correct.
	Verify that the user accounts exist and are accessible.
	Verify that the customer profiles are complete and accurate.
	Verify that the devices and network elements are present.
	Verify that the services for each device are accurate and complete.
	Verify that all of the notification profiles are present.
	Verify that the reports generate and display the accurate historical data.
✓	**Network - Hardware Probes**
	Upgrade your hardware probes by either: • Upgrading automatically through the NAC by clicking Central Server and Hardware Probe Upgrade. Click the following link for the Software Upgrade Mirror Page within the Partner Resource Center: http://www.n-able.com/login/software/upgrade/index.php. Then, copy the appropriate URI for the upgrade you want to perform. For more information, refer to “Setting Up Upgrades” in the *Product Administrator Manual*, or • Burning and installing the most recent Network - Hardware Probe ISO image that can be obtained from the Partner Resource Center.
✓	**Windows Probes**

	Upgrade your Windows probes by either: • At the SO Customer level, selecting Setup Customers. Then select the customers for which you would like to upgrade probes on an individual basis and click Upgrade Probes. On the Upgrade Probes screen, select the required settings, or • Re-installing them to obtain the features of the new Windows-based probes.
✓	**Agents**
	Upgrade your Novell, Linux, and Mac agents manually by accessing the updated agent packages from the N-central Software Download screen.
	Upgrade your Windows agents automatically by setting up the auto-upgrade for all of the agents or for a specific agent. For all of the agents for a specified customer: 1. Sign into the N-central user interface at the SO Customer level. 2. On the menu bar, click Setup>Customers. 3. Select the customers for which you would like to upgrade agents on an individual basis. 4. Click Upgrade Agents. 5. On the Upgrade Agents screen, select the required settings. For a specific agent: 1. Sign into the N-central user interface. 2. On the menu bar, click Setup>Devices. 3. In the Name column, select the appropriate device. 4. Click the Agent tab. 5. In the Update to New Version options, select Now then set to off. If an agent fails to automatically upgrade: • Verify that the agent is configured to automatically upgrade on the Agent tab of the device's configuration screen. • Restart the agent service. Manually upgrade the agent if it does not automatically upgrade after restarting the agent service.
✓	**Branding Profile**
	The branding profile must be updated. Files from the previous version must be removed. For information on which files to remove, please refer to the table Branding Profile Files to Remove for N-central 6.5 on page 19. New files have been included in your N-central 6.5 branding profile. If you would like to brand these files, you must download, customize and upload them through the NAC. For information on files that are new to N-central 6.5, please refer to the table New Branding Profile Files for N-central 6.5 on page 20. For more information on Branding, refer to the online help.

Table 1-2: Branding Profile Files to Remove for N-central 6.5

Files to Remove		
arrow.gif	launch_remote_desktop.gif	scheduled_report_s.gif
background_lines.gif	Lminus.png	service_control_l.gif
blank.png	login_hdr_main_img.jpg	service_custom_l.gif
box.gif	login_ico_web.gif	service_security_l.gif
button_1.gif	login_logo_nableu.gif	service_security.gif
button_wide.gif	login_logo_services.gif	service_voip_l.gif
correlated_notif.gif	login_screen_color.gif	so_level.gif
first.gif	login_spacer.gif	status_l.gif
folder_shared_l.gif	Lplus.png	status.gif
ftr_nable.gif	new.png	T.png
grey.jpg	noc_l.gif	tab_off.gif
help.gif	notif_corr_profile.gif	tab_offWide.gif
I.png	notifications.gif	tab_on.gif
ico_login.gif	overview.gif	tab_onWide.gif
icon_arrow.gif	patch_management_pt.gif	title_bar_bk_off.gif
icon_email.gif	pixel_black.gif	title_bar_bk_on.gif
icon_print.gif	report_bk.gif	Tminus.png
icon_prod_admin_pt.gif	report_cust.gif	Tplus.png
L.png	reports_l.gif	truncated_l.gif
last.gif	reports.gif	truncated.gif

Table 1-3: New Branding Profile Files for N-central 6.5

New Files	
bg_quick_access.gif	map.gif
bg_quick_tab.gif	mapping_info.gif
clone.gif	off_tab_left_on.gif
collapse.gif	off_tab_right_on.gif
collapse_l.gif	preview.gif
expand.gif	rowHighlight.js
expand_l.gif	service_template.gif
favicon.ico	service_template_add.gif
grey.gif	service_template_lg.gif
icon_sort_up_down.gif	service_template_remove.gif
import_unmanaged.gif	smart_folder.gif
job_status_dash.gif	smart_folder_pt.gif
job_status_dash_pt.gif	so_folder.gif
key.gif	so_folder_pt.gif
legacy_asset.gif	whitetip_rollover.gif

Known Problems and Solutions

- Duplicate notifications may be generated for the Windows Event Log service in the following situation:
    - ·If a user clicks OK on any Windows Event Log service screen within a scan interval during which monitored events trigger a notification. This happens even if the user has made no changes to the service.
- Installing Novell agents may fail when using the activation key provided in the UI if the key contains too many characters. If an `Alert - invalid activation key length` error message is displayed during the installation of a Novell agent, use the `load sys:\public\nagent\keydec <activation key from the central server>` command at the Novell console to enter the activation key instead of using the key provided on the Devices screen of the UI. Refer to the “Installing Novell Agents” instructions in the online help for more information.
- Immediately following an upgrade to 6.5.0.x, the Windows Event Log Report will have no data (or incorrect data) in the Date-Time column for the duration of the initial data retention period. Once this period has completed, valid date/time data will be available.
- Due to the merging of services, any existing WTS services will be renamed to HTTP services and any WTSS services will be renamed to HTTPS services.
- The hard drive capacity reported in the Asset Information section of the Device Details screen may be incorrect for larger physical drives (greater than 128GB). This is due to an issue with the manner in which the maximum capacity of physical drives is obtained during asset discovery.
- Asset Discovery may experience issues in some cases when information can not be obtained for a CD-ROM drive which affects the gathering of information for hard drives. If this problem occurs, asset information may be incomplete as hard drive capacity and other information may not be available.
- When logging in, you may receive an error message indicating that the CA Root certificate is not trusted if you are using Internet Explorer 7.0. Click Install Certificate to resolve this error.
- When configuring a Windows Network probe on a system using Windows Vista, firewall settings must be modified to allow WMI as an exception.
- When running Remote Support Manager, you may receive the following error if a service has been interrupted unexpectedly:

  `Remote Support Manager has detected that a software error has occurred.`

  Click Ignore to remove the error message and Remote Support Manager should function normally. Contact Technical Support if this error message is repeated.

- Service settings and thresholds for services assigned to a probe (for example, the Probe Status service) can be modified through the NOC View if the probe is reporting a Stale/Misconfigured/Warning/Failed/No Data status. If the service is in a Normal state, the settings can be changed by doing the following:

  a. Associate the probe to a folder,

  b. Add the folder to a dashboard,

  c. Associate the service to the dashboard, and

  d. Edit the service by clicking on it's status icon in the dashboard.

- If you are using VirusXIT or SpyXIT (McAfee Total Protection for Small Business), they include an anti-spyware tool that blocks Managed Device Remote Control and Remote Desktop Support. For Remote Desktop Support, click Allow when McAfee blocks the attempt. For Managed Device Remote Control, right-click the McAfee icon in the system tray of the target device and select Scan Tasks>View PUP Detections. Then, select all the VNC options listed and click Allow.

  Note: Once McAfee has blocked an attempt on one target device, you can optionally set a global setting of Allow in the web-based portal and apply this setting to all devices. For more information, refer to the McAfee documentation.

- The formatting of e-mail notifications for asset discovery tasks may be inconsistent with some devices listed on one line while others will list multiple devices on the same line. This is due to Microsoft Outlook having issues with line breaks in plain text format. For more information, refer to Microsoft technical documentation available at http://support.microsoft.com/kb/287816.

- Uninstalling and re-installing Remote Support Manager on a device using Remote Environment Manager can cause functionality issues including being able to access Remote Support Manager with a Web browser but not N-central. It is therefore recommended that you do not uninstall and re-install Remote Support Manager using Remote Environment Manager. Should functionality problems occur as a result of this issue, please perform the following steps:

  a. Select Setup > Devices.

  b. Click on the name of the device.

     ↳ The Edit Device screen appears.

  c. Select the Details tab.

  d. Clear Install Remote Support Manager to uninstall Remote Support Manager.

  e. Wait for the uninstall completion notice.

f. Select Install Remote Support Manager to install Remote Support Manager again.

Remote Support Manager should then function properly.

- Due to the differences between the original Event Log service used in older versions of N-central and the new Windows Event Log service available with N-central 6.5, configuration of the service will need to be modified to maintain similar notification patterns. For example, if an Event Log service on an older version of N-central was monitoring multiple options, individual notifications would be sent for each qualifying event. After upgrading to N-central 6.5, individual Windows Event Log tasks would need to be created to monitor specific options in order to result in multiple notifications being sent when multiple triggering events take place.
- N-compass Reporting for N-central: If you intend to use N-compass as your reporting engine, you must complete the following non-required fields when adding a customer to the system: First Name, Last Name. These fields are found in the Contact Information section of the Enter Customer Details screen. Data export will fail if these fields are not completed. If the Customer Wizard was used to create a customer account, you must edit the customer details to add the contact information.
- As a result of modifications made to accommodate localization of exported service template XML files, any service template XML files that were exported using N-central 6.5 Limited Release (Build 6.5.0.304) can not be imported by N-central 6.5.
- Any instances of the Backup Exec, Windows Event Log, IIS, or SQL Server services that were added to devices through service templates using N-central 6.5 Limited Release (Build 6.5.0.304) will have invalid parameter values. After upgrading to N-central 6.5, instances of these services must be deleted and then added to the affected devices again.

Fixed Bugs

The following bugs have been fixed for this release:

Agents and Probes

- An issue concerning Windows probes referring to an incorrect IP Address when downloading the agent installer has been addressed.
- An issue with SO User accounts being able to change the monitoring probe for services has been addressed.
- A problem with the initialization of remote agent installation has been resolved by improvements made to discovery jobs.

- An option has been added to provide proxy configuration of hardware probes instead of having to manually edit the nagent.conf file.
- An issue concerning the reporting of invalid recipe messages during asset discovery has been addressed.
- An issue with probes deploying wrong versions of agents has been addressed.

Central Server

- During activation of the server, all modules are now enabled by default.
- A problem with branding reverting to the default settings instead of retaining customized branding during the re-activation of the server has been addressed.
- N-central self-monitoring of swap thresholds have been set to higher levels.
- The file system capacity has been increased to address upgrade failures that resulted from a full backup file system.
- The backup scripts have been revised to ensure proper FTP transfer of the correct files.
- The N-central internal web server now rotates and compresses all daily logs, including the last log(s) of the day.

Devices

- Improvements with discovery jobs have resolved an issue with the duplication of devices being imported into the device list.
- An issue with the SNMP Version logic resulting in the failure of discovery has been resolved.
- WSUS devices now map correctly to N-central devices.
- Connectivity now does not report Normal on devices that are powered down or disconnected.

NAC

- An issue concerning system backup where the Include Historical Data option was not operating properly has now been addressed.
- The Custom Branding Profile in the NAC contained the branding files for the wrong version (5.x HTML). This issue has been resolved.
- An issue with being unable to set the default parameters for the Windows Event Log service through the NAC has been resolved by removing this function from the NAC. Instead of using the NAC, you can now use a service template in the UI to modify the parameters for this service and then apply the service template (with the modified service) to devices as required.
- When uploading individual branding files, only the appropriate files are listed.

- Custom branding profile images from N-central 6.0 are preserved during the upgrade to N-central 6.5.

Reporting

- An issues with customer names being replaced by dashboard names in the Executive Summary Report has been addressed.
- Monitoring Element Version now returns the last time the agent or probe checked in, in the column, Last Check In.

Services

- An issue concerning the System Change service and its application to discovered devices has been addressed.
- Antivirus protection has been enhanced by the AV — Security Center service supporting Symantec AntiVirus™ Corporate Edition 10.0.
- An issue concerning the use of inappropriate units for unit scaling in Traffic services has been addressed.
- Database maintenance issues concerning the removal or updating of custom services have been resolved.
- An issue concerning the incorrect display of custom headings for the Log Analysis (Appended) service has been addressed.
- An issue with the Backup Exec service using Universal Time Coordinated (UTC, also known as Greenwich Mean Time or GMT) instead of local time has been addressed.
- After upgrading to N-central 5.2, the IIS Service no longer reports as being in a Misconfigured state.
- An issue with the MBSA 2.0 service being unavailable for Windows workstations has been addressed.
- Backup Exec no longer reports Stale status due to text strings longer than 250 characters; longer text strings for scan details are now supported.
- An issue with string cooked type 5 discarding messages instead of truncating them has been addressed.
- An issue has been addressed with the initial value of the `LAST_SCANTIME` parameter for the Backup Exec service not being that of the time of upgrading or installing N-central.
- An issue with the Backup Exec service returning a `Retrieve results not attempted error` has been resolved.

Technical Documentation

- Additional information has been provided in the documentation concerning

correlated notifications.

- An incorrect definition of Active User Count in the documentation of the Exchange Server service has been revised.
- Information has been provided concerning the requirement to log on to a workstation with the same credentials that will be provided when installing a Windows probe.
- Revisions have been made to the probes hint help concerning minimum and maximum disk space values.
- A note has been added identifying that devices running Windows 2000 cannot monitor the Disk Queue Length service.
- Incorrect information in the hint help for the Generic Integer service has been revised.
- Documentation has been added on the use of multiple instances of the Windows Event Log service to provide detailed status reports of multiple log types.
- A 'Branding Image Files List' has been added to the N-central Branding Guide which includes filenames and descriptions of all branding image files.
- A typographical error in the Hint Help for the Remote Desktop Support screen (For Authenticating Proxies field) has been corrected.
- Documentation now indicates that there is 32-bit only support for SuSE Linux 9.1 Professional.

User Interface

- The scaling issue when the Service Metrics report is run on two interfaces has been resolved.
- An issue with the transition between the System Change screen and the Discovery screen has been addressed.
- An issue with accessing the Reports tab from the Edit Device screen has been resolved.
- An issue with the alignment of field titles in the Remote Desktop Support - Contact Details screen has been resolved.
- After custom branding files are uploaded, Chinese characters display correctly.

Other

- Asset discovery discovers local and other drives and reports on drive types.
- An error message concerning the deletion of notification methods that are associated with notification profiles has been clarified.
- An issue with the application of 080-Patch19051.sql failing when the data export log was not empty during the upgrade from N-central 5.0 Service Pack

2, Hotfix 4 to N-central 5.1 has been addressed.

- A new java export tool will update the Auditlog and directly update the syssemaphores database table to report that an export is in progress, even if the export tool is started manually.
- An issue concerning obsolete mgetty entries in the logrotate.d file corrupting the logrotate.status file has been addressed.
- A problem with notifications indicating no data in the database after upgrading to x 5.1.2 has been addressed.
- An issue with NKO not logging to nko.log has been addressed.
- You now have the ability to install a wildcard SSL certificate.
- An issue with TG3 and BNX2 NIC drivers during upgrade has been resolved.
- An issue with upgrading 6.0.0.431 databases to 6.5.0.304 has been resolved.
- Service_20165.xml now uploads during upgrade.
- Installing a Hotfix through Auto Update now works.
- An issue with repetitive re-starting of the N-central internal web server during upgrade has been resolved.

Probe Support Across Different Platforms

Platform	Services				Asset Discovery	Auto-discovery	Script/ Software Distribution
	System	Network		Security			
	Remote WMI	SNMP	TCP	Syslog			
Network Hardware Probe							
N-central Hardware Probe		✓	✓	✓		✓	
Network Windows Probe							
Windows 2003 Server, Windows Small Business Server 2003	✓	✓	✓	✓	✓		✓
Windows 2000 Professional SP4, Server SP4, Advanced Server SP4	✓	✓	✓	✓	✓		✓
Windows XP Professional SP2	✓	✓	✓	✓	✓		✓
Windows Vista Business, Ultimate, Enterprise	✓	✓	✓	✓	✓		✓
Workgroup Windows Probe							
Windows 2003 Server, Windows Small Business Server 2003	✓	✓	✓	✓	✓		✓
Windows 2000 Professional SP4, Server SP4, Advanced Server SP4	✓	✓	✓	✓	✓		✓
Windows XP Professional SP2	✓	✓	✓	✓	✓		✓
Windows Vista Business, Ultimate, Enterprise	✓	✓	✓	✓	✓		✓

-

Agent Support Across Different Platforms

Platform	Services				
	System	Security		VoIP	
	Local API	Local API	Syslog	SNMP	Remote WMI
Windows Agents					
Windows 2003 Server, Windows Small Business Server 2003	✓				
Windows 2000 Professional, Server, Advanced Server	✓				
Windows XP Professional SP2	✓				
Windows Vista Business, Ultimate, Enterprise	✓				
Linux Agents (Veritas and Event Log are not supported)					
RedHat Enterprise Linux AS, ES, WS 3.0 and ES 4.0	✓				
SUSE Linux Professional 9.1 (32-bit version) **Note:** 64-bit version is not supported.	✓				
Novell Agents (Veritas, Event Log, and Local IP are not supported)					
Novell 6.5 SP1a, SP2, SP3, SP4, and SP5	✓				
Mac OSX Agents (Veritas, Event Log, Local IP, Antivirus Activity, and Antivirus Definition are not supported)					
Mac OSX 10.4	✓				

Terms and Acronyms

EDF
External Data Feed is a portal through which data from external application can be submitted to N-central and processed on the dashboard.

MD5
A hashing algorithm used to verify data integrity. Theoretically, no two files will generate the same MD5 signature. By comparing a file's calculated MD5 signature with its known signature, we can detect changes (corruption) in the file.

MD5 Signature
Also known as an MD5 checksum. A 32-character hexadecimal string that uniquely identifies a file. If the file changes or becomes corrupted, the MD5 signature will change.

NAC (N-central Administrator Console)
The administrative interface used to set up and administer the N-central server. Formerly known as the NCSAI.

NCSAI (N-central System Administration Interface)
Now known as the N-central Administrator Console (NAC).

NOC
The Network Operations Center view in N-central can be used to track the active incidents of a network.

ODBC (Open Database Connectivity)
This is an open and standards-based application programming interface, used to access a database. Through an ODBC interface, N-central allows monitored data to be exported to an external reporting tool or data warehouse.

SHA1
The Secure Hash Algorithm is used when the central server database is backed up. It ensures that the database is backup is not corrupted.

Simple Network Management Protocol (SNMP)
This is a protocol that allows a device to be monitored and configured remotely over a network. N-central has provided built-in support for monitoring network interfaces, and for 'custom service' plug-ins that expand its SNMP management capabilities.

WMI

The Windows Management Instrumentation protocol is used by N-central to obtain information on local services of a Windows device.

WSUS

Windows Server Update Services is a Microsoft product that allows full control over the deployment of the latest Microsoft product updates.

Customer Support

Toll Free: 1-866-302-4689

Web Page: www.n-able.com

Technical Support Self-Service Portal: http://www.n-able.com/support/

Copyright © 2007 N-able Technologies.

All rights reserved. This document contains information intended for the exclusive use of N-able Technologies' personnel, partners, and potential partners. The information herein is restricted in use and is strictly confidential and subject to change without notice. No part of this document may be altered, reproduced, or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of N-able Technologies.

Copyright protection includes, but is not limited to, program code, program documentation, and material generated from the software product displayed on the screen, such as graphics, icons, screen displays, screen layouts, and buttons.

N-able Technologies, N-central and Monitor Manage Optimize are trademarks or registered trademarks of N-able Technologies International Inc., licensed for use by N-able Technologies, Inc. All other names and trademarks are the property of their respective holders.